Testimony to Assembly Committees on Consumer Affairs and Protection, Governmental Operations, and Local Governments

Re: Legislature Should Set Statewide Transparency and Oversight Standards for ALPRs, as It Has Already Done for Traffic Enforcement Cameras

November 9, 2026

Thank you for the opportunity to provide written testimony on the use of automatic license plate readers in New York State. Reinvent Albany advocates for transparent and accountable government in New York.

Reinvent Albany strongly supports automated traffic enforcement programs – red light cameras, Automated Camera Enforcement (ACE) on bus routes, and school zone speed cameras – which have decreased violations, increased public safety, and improved bus speeds. State legislation is required for these programs, which include data-sharing and privacy safeguards, and are subject to repeated sunsetting provisions (see the Appendix showing the history of approvals).

Generally speaking, Reinvent Albany supports home rule and recognizes the importance of allowing local governments to make decisions that reflect the needs of their communities. We believe the State should grant localities permanent authority to:

- Set maximum speed limits;
- Create and operate automated traffic enforcement camera programs, including hours of operation, number and type of cameras, locations, and penalties;
- Establish residential parking permit programs; and
- Use automated parking enforcement.

However, for automated license plate readers (ALPRs), the State must establish a baseline of transparency, accountability, and privacy protection – similar to how automated traffic enforcement programs operate under statutory requirements that establish clear purposes, rules, and chains of custody of data. Without these protections, the public cannot trust that the government is using their information properly. We urge the Legislature to pass legislation that requires the following (we note that A10808-A (Hunter) / S9890-A (Hinchey) contains many of these safeguards, which we are currently evaluating):

1. Strict access controls and clear chains of custody of ALPR data;
2. Public reporting of agency use of ALPRs, with independent oversight;
3. Public disclosure of contracts and agreements;
4. Strict limitations on permissible uses and sharing data; and
5. Short data retention limits.

Public Policy Benefits of Automated Traffic Enforcement

We understand that today's hearing focuses on privacy, data sharing, and surveillance. While the Assembly explores these important issues, which we touch on later in this testimony, we believe it is important to note the benefits of current automated traffic enforcement programs:

- **Red Light Cameras have** reduced violations by 80% since 1994. Injuries from rear-end collisions have declined by nearly 60%, and injuries caused by right-angle collisions have declined by 70% since camera installation.
- **Automated Camera Enforcement (ACE) has improved bus speed.** Bus speeds on ACE-equipped routes increased by 5% since 2024, with some corridors seeing gains as high as 30%. These routes have also seen a 20% reduction in collisions and a 40% reduction in bus stops being blocked by vehicles.
- **Speed cameras are working.** Since 2014, speeding at camera locations has dropped by an average of 95%. Pedestrian, cyclist, and motor vehicle occupant injuries have decreased, though the NYC Department of Transportation notes safety benefits have become "less dramatic as speed cameras have become ubiquitous."

ALPRs Lack Safeguards Similar to Current Automated Traffic Enforcement Authorizations

It is important to distinguish between automated traffic enforcement cameras — red light cameras, speed cameras, and ACE bus lane enforcement — and ALPRs. Such automated traffic enforcement cameras are event-triggered and narrow in scope. They activate only when a specific traffic violation occurs, such as running a red light, speeding, or illegally using a bus lane. They are designed to document a particular violation for a specific, limited purpose – not to continuously monitor the movements of everyone who passes by.

New York's automated traffic enforcement laws also establish important privacy protections and oversight mechanisms. The laws require annual reporting,[1] restrict the purposes for which collected information can be used,[2] and prohibit both the collection of biometric or identifying information[3] and the use of facial recognition.[4] The cameras identify only license plates, not individuals, and their use is tied to a specific enforcement purpose, rather than broad, ongoing surveillance.

Because these systems collect such limited information, they also create fewer opportunities for unauthorized access and abuse. Less sensitive data is available to be compromised; it consists solely of the license plates of vehicles committing particular infractions at discrete points in time.

In contrast, ALPRs are a powerful surveillance technology that can collect vast amounts of sensitive data about the public, whether or not they have done anything wrong. Because they operate continuously, information can be aggregated over time into a detailed record of where people travel, where they work, whom they visit, and what places they frequent. The enormous

[1] VAT §§ 1180-b(n), 1111-c(l), 1111-a(m).
[2] VAT §§ 1180-b(a)(5)(ii), 1111-c(a)(3)(ii).
[3] VAT §§ 1180-b(a)(5)(i), 1111-c(a)(3)(i), 1111-a(a)(2).
[4] VAT § 1111-c(a)(3)(iii).

volume of information collected, combined with the ability to search historical location data and share it across jurisdictions, creates the potential for a mass surveillance database of people's movements without any individualized suspicion or evidence of wrongdoing, all hidden from public awareness — a situation that undermines the public's trust in government and is ripe for abuse absent legislative action.

Recommendations for ALPR Transparency and Oversight

Reinvent Albany supports a statutory baseline for ALPR transparency and oversight, similar to how automated traffic enforcement programs operate under statutory requirements that establish clear purposes, rules, and chains of custody of data that outline who has access to ALPR systems and when. Presently, law enforcement agencies often acquire and deploy ALPR systems with little public visibility. Agencies can negotiate contracts and data-sharing arrangements behind closed doors, while the public has limited information about which agencies use the technology, what information they collect, who has access, how long they retain the data, and with whom they share it. The publicmust file repeated Freedom of Information Law requests for this basic information that should be public by default. When government agencies fail to be transparent about their use of ALPRs, they risk eroding confidence in government institutions as the public is left to question whether these technologies are used ethically and legally. That is unacceptable for a technology capable of tracking the public on such a sweeping scale.

Furthermore, private companies increasingly operate ALPRs, creating privately controlled databases that law enforcement can access or purchase. This creates the opportunity for government agencies to circumvent public safeguards by purchasing surveillance data from a private company rather than collecting it themselves. The State also must establish transparency and accountability requirements for these arrangements.

The use of ALPRs should not be left to a patchwork of local policies, law enforcement discretion, or opaque agreements with private vendors that leave New Yorkers in the dark. The State must establish a clear floor of transparency and governance – similar to the requirements around automated traffic and bus enforcement cameras – to ensure that this technology is used only for narrowly defined purposes, with meaningful oversight and public accountability.

At a minimum, New York State must establish the following baseline protections:

1. **Strict access controls and clear chains of custody for ALPR data**: Clear rules must govern who can access ALPR systems and databases, who is authorized to conduct searches, what justification is required, and who approves access. Agencies must regularly review access privileges and revoke them when an employee no longer has a legitimate need. All searches and data access should be logged and subject to audits.

2. **Public reporting of agency use of ALPRs, with independent oversight**: Agencies should be required to disclose:
    a. which ALPR systems they operate and how many devices they deploy;
    b. what purposes they serve;
    c. which agencies they share information with;

d. how frequently the systems are used and how many times they are accessed,
e. who accessed them and who has authorizations for access; and
f. the purpose for which they are accessed.

Without this information, it is impossible to conduct independent audits that can identify misuse and ensure compliance with statutory requirements.

3. **Public disclosure of contracts and agreements**: Agencies should publish ALPR contracts, memoranda of understanding, and data-sharing agreements between agencies on their websites. The public has a right to know what technology its government is purchasing, what capabilities it provides, what data is collected, what restrictions apply, and what obligations vendors have regarding the information – including whether vendors can sell, share, or otherwise repurpose collected data. Government agencies should also be required to publish on their websites contracts governing the purchase of data from private ALPR databases, including the terms of access, the scope and origin of the datasets, when and where the information was collected, and the purpose for which it was acquired.

4. **Strict limitations on permissible uses and sharing data**: ALPR data should only be used for clearly defined, narrowly tailored purposes. Agencies should be prohibited from using the technology for purposes unrelated to the original justification for collecting the data. Data sharing with out-of-state agencies and jurisdictions should be severely restricted, if not prohibited, and limited to clearly defined, narrowly tailored purposes. New Yorkers should not have their movements made accessible to law enforcement entities across the country – entities that may lack New York's safeguards – through loosely governed data-sharing networks.

5. **Short data retention limits**: Non-hit ALPR data (data that is not tied to an ongoing investigation) should be automatically deleted within a short time frame. Retaining information about people with no justification creates an unnecessary record of their movements and breeds distrust in the government's use of personal information.

Many of these safeguards are implemented in A10808-A (Hunter) / S9890-A (Hinchey). While Reinvent Albany is still evaluating the full scope of this bill, we support and urge the Legislature to seriously consider the provisions related to transparency, oversight, and data sharing.

The extraordinary surveillance capabilities of ALPRs demand a consistent statewide baseline. As with the statutory safeguards governing automated traffic enforcement cameras, ALPR use must be subject to clear rules on purpose, access, retention, authorization, and public disclosure. These are necessary protections to ensure that powerful surveillance technology does not undermine civil liberties, government transparency, and public trust in government institutions.

Appendix - Timeline of NYS Authorizations for Automated Enforcement Programs

NYC Red Light Camera Program History of State Authorization		
Year/Date of Legislative Action	**Number of Intersections Authorized**	**Action**
1988	25	Authorized the initial program - Chapter 746
1991	25	Extended the program
1993	25	Extended the program.
1995	50	Expanded to 50 intersections and renewed until December 1, 1999.
1999	50	Extended the program.
2004	50	Renewed until December 1, 2009 - Chapter 667
September 13, 2006	100	Expanded to 100 intersections - Chapter 658
April 28, 2009	150	Expanded to 150 intersections and renewed until December 1, 2014. Chapter 18 of 2009.
July 22, 2014	150	Renewed until December 1, 2019 - Chapter 134
April 12, 2019	150	Renewed until December 1, 2024 - Chapter 58 of 2019, Part TT
October 23, 2024	600	Expanded to 600 intersections and renewed until December 1, 2027 - Chapter 437

See NYC DOT's 2011 Red Light Camera Program Review Report, 1994-2010 for Pre-2000 actions: https://www.nyc.gov/html/records/pdf/govpub/6861rlc_briefing_document_2011.pdf

NYC School Speed Cameras History of State Authorization		
Date of Legislative Action (unless otherwise noted)	**Number of Speed Zones**	**Action**
July 31, 2013	20	Authorization of five-year pilot program - Chapter 189
August 27, 2018 (Executive Order)	*140*	*Enabled NYC to restore the program after authorization lapsed - EO 188*
May 12, 2019	750	Expanded to 750 zones, extended operating hours, and renewed authorization until July 1, 2022 - Chapter 30
June 24, 2022	750	Allowed 24/7 operation and renewed authorization until July 1, 2025 - Chapter 229
June 30, 2025	750	Renewed authorization until July 1, 2030 - Chapter 184

MTA Bus Cameras History of State Authorization		
Date of Legislative Action	**Coverage**	**Action**
June 22, 2010	Six specified SBS corridors	Authorized the initial bus-lane camera pilot until September 20, 2015 - Chapter 59 of 2010, Part II
September 18, 2015	Original corridors plus up to 10 additional routes	Expanded eligible routes and renewed authorization until September 20, 2020 - Chapter 239 of 2015
April 12, 2018	Same route cap	Expanded operating hours to 6 a.m.–10 p.m. and authorized at least 50 bus-mounted cameras on eligible Manhattan routes below 96th Street - Chapter 59 of 2018, Part NNN
June 24, 2019	All NYC bus lanes; no route cap	Removed the route cap and time restrictions; renewed authorization until September 20, 2025 - Chapter 39 of 2019, Part D
May 3, 2023	No route or camera cap	Authorized broader ACE enforcement, including blocked bus stops and double parking, and extended bus-camera authorization until July 1, 2028. Chapter 56 of 2023, Part MM